CB-BEITRAG

Dr. Jochen Notholt, RA, und Udo Steger, RA

Step-by-Step: Compliance-Risiken beim Einsatz von Cloud Computing in Unternehmen

Ziel dieses Beitrags ist es, einen Überblick über die wesentlichen Compliance-Risiken zu geben, die nach deutschem Recht beim Einsatz von Cloud Computing zu beachten sind. Der Beitrag versteht sich als „Checkliste" und damit als Entscheidungshilfe für Unternehmen, in denen über den Einsatz von Cloud-Angeboten nachgedacht wird. Anhand von Kontrollfragen lässt sich abschätzen, welche Risiken bei der Entscheidung für die Nutzung eines Cloud Computing Dienstes zu berücksichtigen sind. Zugleich können Anbieter von Cloud Leistungen anhand dieses Beitrags prüfen, wie attraktiv ihre Leistungen für potentielle Kunden sind, die das Thema Compliance ernst nehmen.

1 Was ist und was bedeutet Cloud Computing?

Nach dem ersten Hype befindet sich Cloud Computing derzeit in einer interessanten Phase, man könnte auch sagen: am Scheideweg. Einerseits haben sich Cloud-Angebote zu einer kommerziell reizvolle Alternative zur herkömmlichen IT-Nutzung im Unternehmen am Markt entwickelt, und etablierte IT-Anbieter richten ihre Strategien zunehmend an Angeboten „aus der Cloud" aus. Andererseits hat nicht zuletzt die aktuelle Berichterstattung um die Internetüberwachung internationaler Geheimdienste vermutlich Einfluss auf das Risikobewusstsein in deutschen Unternehmen, was die künftige Nutzung von Cloud Computing betrifft.

Für die Zwecke dieser Betrachtung lässt sich „Cloud Computing" beschreiben als die flexible Bereitstellung von IT-Ressourcen aus einem geographisch verteilten und mit den anderen Nutzern zumindest physisch geteilten Pool, die über Datennetze, i. d. R. das Internet, genutzt werden, und die Vergütung meist abhängig vom quantitativen oder zeitlichen Umfang der Nutzung erfolgt. „IT-Ressource" kann sowohl die Bereitstellung einer Standardsoftware als auch von Hardware sein, wobei einzelne Gestaltungsformen nicht immer klar abgegrenzt werden können.

Immer öfter nehmen Unternehmen Cloud Leistungen wahr, meist um bisher selbst intern bereitgestellte IT-Leistungen zu ersetzen. Manche Standardsoftware kann sogar nur noch im Wege des Cloud Computing bezogen werden. Dies wird auch durch Rechtsprechung wie die „Used Soft" Entscheidung des EuGH (3.7.2012 – C-128/11, EWS 2012, 328, K&R 2012, 493, RIW 2012, 785, WRP 2012, 1074) gefördert, wonach nur noch der Vermieter manche weitgehende Nutzungsbeschränkung an einer Software durchsetzen können soll.

Wir nehmen für diesen Beitrag an, dass ein Unternehmen, das Cloud Leistungen beziehen möchte („Cloud Kunde") in Bezug auf die bisher selbst bereitgestellten und zukünftig vom Cloud Computing umfassten IT-Leistungen alle erforderlichen Maßnahmen zur IT-Compliance ergriffen hat. Die im Folgenden dargestellten Risiken basieren daher allesamt auf dem Umstand, dass ein Cloud Kunde beim Einsatz von Cloud Computing zumindest Teile seiner IT-Ressourcen und seiner Daten aus der Hand – nämlich in die Hand des Cloud Anbieters – gibt. Anders als beim „klassischen" IT-Outsourcing bleiben dabei jedoch die IT-Ressourcen und Daten gerade nicht physisch beim Cloud Kunden. Natürlich gilt auch: Ist der zukünftige Cloud Kunde bislang nicht „IT-compliant", wird dies in aller Regel auch durch den Einsatz von Cloud Computing nicht gelingen.

2 Vertragliche Risiken

Rechtliche Risiken beim Cloud Computing werden oft nur mit Blick auf Risiken aus dem Datenschutz und den drohenden Bußgeldern diskutiert. Das ist aber nur ein Aspekt, den Cloud Kunde und Cloud Anbieter berücksichtigen müssen. Auch aus den anderen vertraglichen Regelungen können sich erhebliche Risiken ergeben (Step 2, 1.). Häufig berücksichtigen zukünftige Cloud Kunden auch zu wenig, dass sie selbst Dienste gegenüber ihren (End-)Kunden erbringen und für die dabei erhaltenen Daten ihrer (End-)Kunden die Verantwortung tragen und teilweise auch ihren Weisungen unterworfen sind. Ebenso sind besondere Vorkehrungen zu treffen, wenn die Cloud Leistungen Teile der kritischen Infrastruktur des Cloud Kunden darstellen. Dies sollte beim Vertrag mit dem Cloud Anbieter besonders berücksichtigt werden (Step 2, 2.).

1. Vertrag mit dem Cloud Anbieter

a) Vertragspartner und Leistungserbringer

In der Praxis trifft man gelegentlich auf Anbieter, die zwar die Cloud Leistungen erbringen, jedoch nicht direkter Vertragspartner des Cloud Kunden werden (möchten). Stattdessen soll ein wirtschaftlich meist schwächerer Dritter, z. B. ein Vertriebspartner, in eigenem Namen den Vertrag mit dem Cloud Kunden schließen. Häufig soll

der Kunde parallel zum Cloud Vertrag noch „Nutzungsbedingungen“ des Cloud Anbieters akzeptieren. Spielraum für Verhandlungen gibt es dabei kaum. Es liegt auf der Hand, dass solche Konstellationen besonders risikoreich und damit sorgfältig zu prüfen sind.

Kontrollfragen:
- Ist der Cloud Anbieter zugleich Vertragspartner? Wenn nein, ist transparent, welche Partei Vertragspartner ist? Sind bei mehreren Parteien auf Anbieterseite die Verantwortlichkeiten klar verteilt?
- Ist klar geregelt, wer Ansprechpartner bei Problemen mit den Cloud Leistungen ist? Sind die Kommunikationswege klar geregelt und aus technischer und organisatorischer Sicht für den Cloud Kunden akzeptabel?
- Falls der Cloud Anbieter nicht zugleich Vertragspartner ist: Wird deutlich, welche Gründe es für diese Rollenverteilung gibt? Hierbei ist zu beachten, dass ein Vertragspartner, der nicht der Anbieter ist, bei Leistungsmängeln womöglich Schwierigkeiten haben wird, Abhilfe zu schaffen. Zu bedenken ist zudem, dass der Kunde vor dem Fall der Insolvenz und Geschäftsaufgabe *aller Beteiligten* geschützt sein muss.

b) Unterauftragnehmer

Cloud Anbieter erbringen die Leistungen häufig durch Unterauftragnehmer innerhalb und außerhalb ihres Konzernverbunds. Dadurch kann die Leistungserbringung für den Cloud Kunden zusätzlich intransparent werden.

Kontrollfragen:
- Sind im Vertrag die Unterauftragnehmer des Cloud Anbieters ausdrücklich benannt?
- Kann der Cloud Anbieter (weitere) Unterauftragnehmer ohne Zustimmung des Cloud Kunden einsetzen? Kann sich der Cloud Kunde dagegen wehren, wenn z. B. einer seiner Wettbewerber als Unterauftragnehmer tätig werden soll?
- Verpflichtet sich der Cloud Anbieter dazu, eventuelle Unterauftragnehmer seinerseits entsprechend seiner eigenen vertraglichen Verpflichtungen zu verpflichten? Kann der Cloud Kunde dies nachprüfen?
- Hat der Cloud Anbieter hinreichende Vorkehrungen für den Fall getroffen, dass Unterauftragnehmer ausfallen?

c) Leistungsumfang, Leistungszusagen und Preismodell

Cloud Leistungen werden i. d. R. in standardisierter Form bereitgestellt. Kundenindividuelle Anpassungen sind, von einfachen Parametrierungen abgesehen, in aller Regel nicht möglich. Cloud Anbieter sind daher meist auch nicht bereit, wesentliche Änderungen an den Vertragsbedingungen zu akzeptieren. Daher ist genau zu prüfen, ob die Cloud Leistungen in der Form bereitgestellt werden, die der Cloud Kunde benötigt, etwa im Hinblick auf Funktionalitäten (z. B. von Software), Performance, Verfügbarkeiten, Wartung/Support, Nebenleistungen (wie z. B. die Datensicherung) und Preismodell. Dazu gehört auch die Prüfung, ob eine Standardlösung ausreicht, um alle wesentlichen Anforderungen des Cloud Kunden abzudecken.

Kontrollfragen:
- Ist der Cloud Anbieter zur Erfüllung klar definierter Leistungszusagen verpflichtet, oder ist der Vertrag in dieser Hinsicht weich formuliert („best effort“ Prinzip, etc.)?
- Besteht die Möglichkeit, die Cloud Leistungen quantitativ und qualitativ kurzfristig zu erweitern oder zu reduzieren? Sind Preisbänder oder andere Schwellen zu beachten?
- Behält sich der Cloud Anbieter das Recht vor, seine Leistungen ohne Zustimmung oder Widerspruchsmöglichkeit des Cloud Kunden zu ändern? Gibt es zumindest eine Vorabinformation, und wenn ja, mit welcher Frist? Wird ein Sonderkündigungsrecht eingeräumt?
- Ist das Preismodell verständlich und beschreibt alle wahrscheinlich in Frage kommenden Leistungen? Gibt es unklare oder versteckte Kosten und/oder Preisanpassungsrechte?

d) IT-Sicherheit und Datensicherheit

Cloud Anbieter werben häufig damit, eine höhere Datensicherheit bieten zu können, als sie der Cloud Kunde selbst gewährleisten könne. Zusagen des Anbieters zur IT-Sicherheit und Datensicherheit (i. S. v. § 9 BDSG und der zugehörigen Anlage) sind aber nicht nur für personenbezogene Daten relevant. Entsprechende Anforderungen gelten für alle betriebsrelevanten Daten, die ein Unternehmen verarbeitet (vgl. nur die „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS)“, Schreiben des BMF vom 28.7.1995 – IV A 8 – S 0316 – 52/95, dort Abschn. 5.)

Zur besseren Übersicht verweisen wir hinsichtlich der Kontrollfragen in den entsprechenden Bereich der Datenschutz-Risiken (s. Step 3).

e) Leistungsstörungen, Rechtsdurchsetzung

Leistungsversprechen des Cloud Anbieters (Step 2, 1.c)) sind nur etwas wert, wenn ihre Nichterfüllung faktisch auch sanktionierbar ist. Diese Frage hängt einerseits davon ab, wie klar der Vertrag die Rechte des Cloud Kunden bei Leistungsstörungen regelt, andererseits davon, ob eine einfache Rechtsdurchsetzung durch den Cloud Kunden möglich ist.

Kontrollfragen:
- Regelt der Vertrag klar und transparent die Rechte des Cloud Kunden für alle für ihn relevanten Leistungsstörungen (z. B. Funktionalitäts- und sonstige Nutzungseinschränkungen, Verfügbarkeitsmängel, Datenverlust und -manipulation, Verstoß gegen sonstige Pflichten wie z. B. Datenschutz-Compliance)? Orientieren sich die Rechte des Kunden an den gesetzlichen Mängelrechten oder gehen sie darüber hinaus?
- Stehen der Geltendmachung dieser Rechte besondere Hindernisse im Weg (z. B. Eskalationsprozeduren, Nachweispflichten für Schäden)? Kann in der Praxis der Nachweis schwerfallen, ob Leistungsmängel in der Verantwortlichkeit des Cloud Anbieters liegen, oder ob sie einen Bereich außerhalb seiner Verantwortung betreffen (z. B. die Netzinfrastruktur)?
- Wie groß ist das Risiko, dass die Leistungen nicht zur Verfügung stehen, ohne dass dies dem Cloud Anbieter anzulasten ist (v. a. im Falle des Ausfalls der Netzinfrastruktur)? Gibt es in diesem Fall andere Parteien, die für die Leistungsstörung ver-

antwortlich gemacht werden können, oder wurden entsprechende Versicherungen abgeschlossen?
- Enthält der Vertrag angemessene und transparente Regelungen zur Haftung des Cloud Anbieters für Sach- und Vermögensschäden des Cloud Kunden?
- Für den Fall, dass der Cloud Kunde bei Leistungsstörungen (oder aus anderen Gründen) Zahlungen zurückhält: Behält sich der Cloud Anbieter in diesen Fällen das Recht vor, Leistungen zu verweigern, Accounts zu sperren oder gar Daten zu löschen?
- Stellt der Cloud Anbieter schriftliche und eigenhändig unterschriebene Vertragsunterlagen zur Verfügung?
- Gilt für den Vertrag deutsches Recht und ein Gerichtsstand in Deutschland? Kann der Cloud Kunde ansonsten schnell und effektiv einstweiligen Rechtsschutz erlangen und auch vollstrecken?

f) Vertragsbeendigung und (Re-)Migration

Ähnlich wie beim IT-Outsourcing muss zwingend schon vor Beginn der Nutzung von Cloud Leistungen definiert sein, was passiert, wenn die Nutzung endet. Zum einen umfasst dies die Mechanismen zur ordentlichen und außerordentlichen Beendigung des Vertrages. Zum anderen ist dies kritisch für die tatsächliche Möglichkeit des Cloud Kunden, zu einem anderen Anbieter zu wechseln oder ggf. die Leistungen wieder selbst zu erbringen („Insourcing"). Schon unter Gesichtspunkten des Risikomanagements muss die Möglichkeit bestehen, den Cloud Anbieter im Falle von Problemen jederzeit kurzfristig verlassen zu können. Umgekehrt sollte es dem Anbieter nicht zu leicht gemacht werden, die Leistungserbringung einzustellen. Eine kurzfristige Migration zu einem anderen System ist praktisch nur selten möglich.

Kontrollfragen:
- Mit welchen Fristen können beide Parteien ordentlich kündigen? Gibt es eine Mindestvertragslaufzeit?
- Gibt es eindeutige und transparente Regelungen, wann der Vertrag „aus wichtigem Grund", also außerordentlich gekündigt werden kann? Sind diese Kriterien so klar, dass der Cloud Kunde ausreichend vor ungerechtfertigten Kündigungen geschützt ist?
- Gibt es Sonderkündigungsrechte des Kunden in besonderen Situationen, z. B. Beauftragung von Wettbewerbern als Subunternehmer des Anbieters oder bei einseitigen Änderungen?
- Regelt der Vertrag transparent und i. S. d. Cloud Kunden die Möglichkeiten zur Remigration der verarbeiteten Daten? Werden vom Kunden in diesem Fall Mitwirkungshandlungen verlangt, die klar definiert sind und die er auch tatsächlich erbringen kann?
- Regelt der Vertrag, dass der Cloud Anbieter die Leistungen auch bei erheblichen Leistungsstörungen auf Seiten des Cloud Kunden weiter erbringen muss, und sei es unter bestimmten Voraussetzungen, z. B. Vorkasse?
- Regelt der Vertrag, dass die Cloud Leistungen notfalls auch nach Vertragsende weiter erbracht werden können, z. B. bei einer Verzögerung der Migration?
- Ist ein Format für die Datenherausgabe vereinbart? Sind die Einrichtungen zum Download leistungsfähig genug? Können überhaupt alle Daten heruntergeladen werden?
- Gibt es eine Möglichkeit zum jederzeitigen Datenexport, d. h. unabhängig von bestimmten vertraglich geregelten Fällen?
- Ist der Cloud Kunde intern auf den Fall vorbereitet, dass die Cloud Leistungen kurzfristig aufgegeben werden müssen? Ist dies notfalls auch ohne Unterstützung durch den Cloud Anbieter möglich, z. B. anhand von Backups?

g) Insolvenz

Das kürzlich in die InsO eingeführte Schutzschirmverfahren soll die Restrukturierung von in die Krise geratenen Unternehmen erleichtern. Das wäre aber für einen Cloud Kunden in der Krise nicht mehr möglich, wenn für den Betrieb des Unternehmens kritische Cloud Leistungen nicht mehr zur Verfügung stehen, weil der Cloud Anbieter schon bei nur drohender Insolvenz den Vertrag kündigt. Der Cloud Kunde sollte daher vertragliche Vorkehrungen treffen, damit er sicher sein kann, in Krisensituationen die Cloud Leistungen weiter in Anspruch nehmen zu können.

Umgekehrt könnte auch der Cloud Anbieter in die Insolvenz geraten und Leistungen einstellen. Dann sollte der Cloud Kunde in der Lage sein, zügig zu migrieren.

Besonders gefährlich sind dabei Dreieckskonstellationen (siehe Step 2, 2.). Wird der Dritte insolvent und fließt an den Dritten bezahltes Entgelt in dessen Insolvenzmasse, könnte der eigentliche Cloud Anbieter mangels eingehender Vergütung schlicht die Leistungen einstellen. Der Cloud Kunde hingegen hat dann faktisch gegenüber keinem der beiden Anderen eine Handhabe.

Kontrollfragen:
- Ist im Vertrag vorgesehen, dass bereits bei nur drohender Insolvenz oder im Falle der Insolvenzanmeldung die Möglichkeit zur fristlosen Kündigung besteht? Falls ja, ist vertraglich vorgesehen, dass die Kündigung abgewendet werden kann, z. B. durch Vorauszahlung?
- Ist das Recht des Cloud Kunden gesichert, im Falle der Insolvenz des Cloud Anbieters auf seine Daten, Datensicherungen und ggf. Dokumentationen zuzugreifen?
- Ist die Portierbarkeit der Daten des Cloud Kunden auf Systeme eines anderen Anbieters oder zurück zum Cloud Kunden vertraglich unter allen Umständen abgesichert und technisch so genau beschrieben, dass die Portierung ohne größeren Konversionsaufwand möglich ist?
- Gibt der Cloud Anbieter bei einer Dreieckskonstellationen (siehe Step 2, 2.) gegenüber dem Cloud Kunden eine Erfüllungsgarantie für den Fall der Insolvenz seines Vertriebspartners?

2. Verträge des Cloud Kunden mit Dritten

Viele Cloud Kunden erhalten personenbezogene Daten und andere vertrauliche Informationen von ihren (End-)Kunden. Oftmals haben sie dafür auch eine besondere rechtliche Verantwortung; dies gilt etwa für Telekommunikationsdienstleister oder Auftragnehmer der öffentlichen Hand. Bei Pflichtverletzungen drohen oft empfindliche Sanktionen. Die Nutzung von Cloud Leistungen sollte daher nicht zu einer Pflichtverletzung führen und muss sowohl Sicherheit als auch Vertraulichkeit dieser Informationen gewährleisten.

a) Geheimhaltungsvereinbarungen

Häufig werden bereits im Vorfeld einer Zusammenarbeit Vertraulichkeitsvereinbarungen abgeschlossen. Darin ist häufig ausdrücklich definiert, was als „vertrauliche Information" gelten soll und wann eine Verletzung der Vertraulichkeitspflicht gegeben ist. Das ist regelmäßig bei unbefugter Weitergabe an Dritte der Fall. Vertraulichkeitsvereinbarungen wirken oft auch deutlich über das Ende vertraglicher Beziehungen hinaus.

Die Speicherung der Daten beim Cloud Anbieter, also bei einem Dritten, kann eine Verletzung der Vertraulichkeitsverpflichtung darstellen. Typische Sanktionen sind etwa Vertragsstrafen oder Sonderkündigungsrechte der anderen Partei, zudem könnten die Straftatbestände der §§ 17, 18 UWG erfüllt sein. Regelungen im Vertrag, wonach in Zweifelsfällen die Zustimmung der anderen Seite einzuholen sei, sind bei einer Migration der geschützten Datenbestände „in die Cloud" nur scheinbar eine Lösung, denn bei einer oftmals unüberschaubaren Zahl von Verträgen und Vertraulichkeitsvereinbarungen ist das praktisch kaum umsetzbar.

Sofern diesen Risiken durch eine Verschlüsselung der vertraulichen Daten begegnet werden soll, ist darauf zu achten, dass die Daten nicht nur verschlüsselt zum Cloud Anbieter transportiert werden, sondern dort auch verschlüsselt gespeichert bleiben (sog. End-to-End Verschlüsselung), und dass der Cloud Anbieter somit keine Möglichkeit hat, die Daten zu entschlüsseln.

Kontrollfragen:
- Enthalten die Verträge des Cloud Kunden mit (End-)Kunden und anderen Vertragspartnern Regelungen zur Vertraulichkeit? (Dies gilt womöglich auch für bereits beendete Vertragsverhältnisse, für die die Vertraulichkeitsverpflichtung fortwirkt und deren Daten vom Cloud Anbieter verarbeitet werden.) Falls ja, werden Vertraulichkeitspflichten des Unternehmens aus diesen Regelungen durch die Nutzung des Cloud Dienstes verletzt? Falls ja, welche Sanktionen sehen die Verträge vor?
- Falls Daten beim Cloud-Anbieter verschlüsselt werden können: Ist die Verschlüsselung so umgesetzt, dass der Cloud-Anbieter keine Möglichkeit hat, die Daten zu entschlüsseln?

b) Datenschutz

Soweit der Cloud Kunde personenbezogene Daten seiner (End-)Kunden im Auftrag verarbeitet, kann er Beschränkungen beim Einsatz von Unter-Auftragnehmern unterliegen, jedenfalls dann, sofern diese nicht gänzlich untergeordnete Tätigkeiten erbringen. Entsprechendes gilt auch bei der Verarbeitung anderer geschützter Datenarten, z. B. von Sozialdaten i. S. d. § 67 SGB X.

c) Sonstige Vertraulichkeitspflichten

Verträge mit (End-)Kunden können auch besondere Vorschriften zum Einsatz von Subunternehmen sowie besondere Vertraulichkeitspflichten enthalten. Das ist typischerweise dann der Fall, wenn der Cloud Kunde mit Kunden umgeht, in denen Daten besondere wirtschaftliche und politische Bedeutung haben, z. B. Banken, öffentliche Verwaltung und der militärische Sektor. Insbesondere öffentliche Auftraggeber verlangen die Einhaltung besonderer Standards hinsichtlich Datenschutz und Datensicherheit, etwa der vom Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichten Standards. Ist die Verlagerung von Leistungen auf Dritte vertraglich untersagt, oder genügt der Cloud Anbieter als Unterauftragnehmer den vom Endkunden geforderten Standards nicht, können dem Cloud Kunden im Verhältnis zu diesem Endkunden je nach Vertragsgestaltung ernsthafte Sanktionen drohen.

3 Datenschutz

Cloud Computing stellt eine besondere Herausforderung für die Gewährleistung des Datenschutzes dar. Allerdings sind die Anforderungen nicht grundverschieden von denen, die sich auch beim IT-Outsourcing stellen. Insofern sollten die nachfolgenden Aspekte und Kontrollfragen als Ergänzung zu den Prüfungen verstanden werden, die jeder Einsatz eines externen IT-Anbieters mit sich bringt.

1. Personenbezogene Daten – überall

Datenschutz-Risiken bestehen zwar nur insoweit, wie der Cloud Kunde vom Cloud Anbieter personenbezogene Daten (§ 3 Abs. 1 BDSG) verarbeiten lässt. Wegen der sehr weiten Auslegung des Begriffs sind in der Praxis jedoch fast immer personenbezogene Daten betroffen. Ausgenommen sind höchstens Konstellationen, in denen der Kunde bereits verschlüsselte oder „anonyme" Daten an den Cloud-Anbieter überträgt – und dies gilt auch nur, wenn man im Gegensatz zu den Aufsichtsbehörden der sog. subjektiven Theorie folgt, wonach es für die Frage des Personenbezugs von Daten auf die subjektive Kenntnis des Einzelnen ankommt. Ebenso ist zu beachten, dass als „anonym" angesehene Daten (§ 3 Nr. 6 BDSG) durch ihre Speicherung in der Cloud re-identifizierbar werden könnten, etwa weil der Cloud Anbieter zusätzliche Informationsquellen hat. In jedem Fall sollten jedoch die oben skizzierten Anforderungen an die Verschlüsselung beachtet werden (oben Step 2, 2. a)).

2. Einhaltung der anwendbaren Datenschutzgesetze durch Cloud-Anbieter

Wir nehmen für diese Checkliste an, dass der Cloud Kunde zur Einhaltung zumindest der deutschen Datenschutzgesetze (v. a. des BDSG, in absehbarer Zeit möglicherweise statt dessen der EU-Datenschutz-Grundverordnung) verpflichtet ist. Wenn er seine (personenbezogenen) Daten nun an den Cloud Anbieter zur Verarbeitung weitergibt, ist er i. d. R. dafür verantwortlich, dass die Verarbeitung durch den Cloud Anbieter gesetzeskonform erfolgt, dieser also die deutschen Datenschutzgesetze einhält. Hierzu sollte sich der Cloud Anbieter eindeutig verpflichten. Idealerweise sollte der Vertrag die Verletzung dieser Pflicht für den Cloud Anbieter mindestens im gleichen Maße sanktionieren, wie es dem Kunden von Seiten der zuständigen Behörden oder auch (End-)Kunden droht. Mittlerweile steigt auch das Risiko, von Wettbewerbern erfolgreich wegen Verletzungen von Datenschutzvorschriften in Anspruch genommen zu werden, vgl. z. B. OLG München, 12.1.2012 – 29 U 3926/11.

a) Verpflichtung von Mitarbeitern und Subunternehmern

Nicht nur der Cloud Anbieter muss sich zur Einhaltung der anwendbaren Datenschutzgesetze verpflichten, sondern auch seine Mitarbeiter und Subunternehmer müssen „mitziehen".

Kontrollfragen:
- Sichert der Cloud-Anbieter vertraglich zu, dass er seine Mitarbeiter auf das Datengeheimnis (§ 5 BDSG) verpflichtet hat?
- Sichert der Cloud-Anbieter zu, dass er nur Subunternehmer beschäftigt, die sich ihm gegenüber im gleichen Umfang zur Einhaltung der Datenschutzregeln auch aus dem Cloud Vertrag verpflichten, wie der Cloud Anbieter gegenüber dem Cloud Kunden verpflichtet ist?
- Sind Konzernunternehmen ebenso verpflichtet wie sonstige Dritte?

b) Auftragsdatenverarbeitung, § 11 BDSG

Nach wohl herrschender Auffassung unter den Aufsichtsbehörden und Praktikern ist Cloud Computing i. d. R. als Auftragsdatenverarbeitung unter den Voraussetzungen des § 11 BDSG zulässig.

Kontrollfragen:
- Ist der Cloud Anbieter bereit, einen gesonderten Vertrag nach § 11 BDSG mit dem Cloud Kunden abzuschließen? Falls ja, stellt er eigene Vertragsmuster zur Verfügung, die den Anforderungen des § 11 BDSG genügen und die keine überraschenden Regelungen zum Nachteil des Cloud Kunden beinhalten? Falls nein, ist er bereit, Vertragsmuster des Cloud Kunden zu akzeptieren oder über seine eigenen Regelungen zu verhandeln?
- Kann der Cloud Anbieter überhaupt zusichern, dass die Daten des Cloud Kunden unter der Kontrolle des Cloud Kunden bleiben und so verarbeitet werden, wie der Cloud Kunde es wünscht – insbesondere tatsächlich gelöscht werden, wenn der Cloud Kunde es wünscht?
- Sichert der Cloud Anbieter zu, nach Vertragsende die Daten des Cloud Kunden endgültig zu löschen und dies auch zu bestätigen?

c) Internationaler Datentransfer

Kennzeichnendes Merkmal von Cloud Leistungen ist es, dass gerade *keine* an geographischen Grenzen orientierte ortsgebundene Datenverarbeitung und -speicherung erfolgt. Vielmehr können die Daten praktisch überall dort auf der Welt gespeichert sein, wo der Cloud Anbieter Rechenzentren betreibt oder betreiben lässt. Dabei können die Daten jederzeit von einem Rechenzentrum ins nächste kopiert oder verschoben werden. Dem gegenüber steht die datenschutzrechtlich erforderliche Kontrolle über die Daten von Daten durch den Cloud Kunden. Die Aufsichtsbehörden fordern, dass der Cloud Kunde zumindest wissen müsse, welche Orte für die Datenspeicherung in Frage kommen.

Regelmäßig gilt dabei ein den deutschen Datenschutzanforderungen genügendes Datenschutzniveau nur dann als gewährleistet, wenn die Datenverwendung ausschließlich in einem der EU- bzw. EWR-Mitgliedsstaaten stattfindet oder in einem der als „sichere Drittstaaten" zugelassenen Ausnahmen, z. B. der Schweiz.

Kontrollfragen:
- Gibt es vertragliche Zusagen des Cloud Anbieters zu den (Stand-)Orten der Datenverarbeitung und zur Benachrichtigung über etwaige Änderungen bzw. das Hinzufügen weiterer Orte? Dazu gehören insbesondere auch die Standorte eventueller Subunternehmer.
- Falls der Cloud Anbieter in den USA ansässig ist: Ist er Teilnehmer am „Safe Harbor"-Programm und erfolgt die Datenverwendung ausschließlich in Rechenzentren in den USA? Falls ja, erlaubt es der Cloud Anbieter dem Kunden, die Einhaltung der „Safe Harbor"-Kriterien gemäß dem Beschluss des Düsseldorfer Kreises vom 28./29.4.2010 zu prüfen?
- Ist der Cloud Anbieter bereit, mit dem Cloud Kunden Verträge auf Grundlage der EU-Standardvertragsklauseln abzuschließen?

d) Technisch-organisatorische Maßnahmen

Ein zentraler Aspekt zur Erfüllung von Datenschutz-Compliance ist die Einhaltung der Anforderungen zur Datensicherheit nach § 9 BDSG und der zugehörigen Anlage durch den Cloud Anbieter. Grundsätzlich gelten dabei die gleichen Anforderungen wie bei einem IT-Outsourcing, ergänzt um einige bei Cloud Computing besonders relevante Fragen.

Kontrollfragen:
- Hat der Cloud Anbieter mindestens dem Stand der Technik entsprechende Sicherungsmaßnahmen ergriffen, um die Mandantenfähigkeit seiner Systeme und damit die Vertraulichkeit der Daten des Cloud Kunden zu gewährleisten?
- Hat der Cloud Anbieter entsprechende Maßnahmen implementiert, die einen unbefugten, unbeabsichtigten, oder technisch fehlerhaften Zugang zu seiner Cloud verhindern, sei es durch Private oder durch Behörden? Gibt es Verfahren zur Meldung und Beseitigung etwaiger Mängel?
- Werden beim Zugriff auf die Cloud und bei der Speicherung der Daten Verschlüsselungsverfahren eingesetzt, die aktuell als sicher gelten?
- Hat der Cloud Anbieter die Verfügbarkeit seiner Cloud abgesichert, etwa durch redundante Datenhaltung oder Maßnahmen gegen Denial of Service Angriffe?
- Hat der Cloud Anbieter seine technisch-organisatorischen Maßnahmen ausführlich und nachvollziehbar dokumentiert, und wird der Cloud Kunde aktiv über Änderungen dieser Maßnahmen unterrichtet?

e) Zertifizierung der Datenschutzkonformität

Direkt beim Cloud Anbieter kann sich der Cloud Kunde meist nicht oder nur unter großem Aufwand von der vertragsgemäßen Verarbeitung der Daten überzeugen, obwohl dies eigentlich nach § 11 BDSG vorgesehen ist.

Kontrollfragen:
- Gibt es eine tatsächliche Kontrollmöglichkeit des Cloud Kunden über die Datenverarbeitung (Verfahren und Ort)?
- Gibt es aktuelle Nachweise bzw. Zertifikate von unabhängigen Stellen über die Standards, denen die Infrastruktur des Cloud Anbieters genügt? Sind diese Nachweise aussagekräftig und erlauben es dem Cloud Kunden, sich einen umfassenden Eindruck von den Maßnahmen zur Datensicherheit zu verschaffen? Gibt es entsprechende Nachweise, wie der Cloud Anbieter die Kontrolle über eventuell eingebundene Unter-Auftragnehmer ausübt?

f) Staatliche Zugriffe

Die Zugriffsmöglichkeiten von Behörden bei Cloud Anbietern gehen teilweise sehr weit. Soweit Zugriffe auf gesetzlicher Grundlage erfolgen, hat ein Cloud Kunde außerhalb von technischen Maßnahmen wie z. B. Verschlüsselung nur dann eine Möglichkeit, hiergegen Rechtsschutz zu erlangen, wenn er über solche Zugriffe rechtzeitig informiert wird.

Kontrollfragen:
- Stellt der Cloud Anbieter nachvollziehbar dar, was er im Fall von behördlichen Anfragen, die die Daten des Cloud Kunden betreffen, unternimmt und welchen Anfragen und Anfragern er sich besonders verpflichtet fühlt (z. B. dem „Patriot Act")? Informiert er den Cloud Kunden über Anfragen? Welche Schritte unternimmt er, um eine Weitergabe zu verhindern?
- Gibt es „Masterkeys" zur Umgehung interner Verschlüsselung oder andere Wege, auf denen Behörden ohne nochmalige Einschaltung des Cloud Anbieters, aber mit dessen Wissen, auf Daten in seiner Cloud zugreifen können?

4 Steuer-/Buchführungs-/Wirtschaftsprüfungs-Risiken

Risiken dieser Kategorie können sich verwirklichen, wenn die beim Cloud Anbieter verarbeiteten Daten Gegenstand handelsrechtlicher oder steuerlicher Aufbewahrungspflichten sind. Dies kann nicht nur bei Cloud-basierten Buchführungs- und ERP-Systemen der Fall sein, sondern auch bei E-Mail, denn E-Mails können direkt (z. B. bei elektronisch übermittelten Rechnungen) und indirekt (z. B. wenn sie Hintergrundinformationen zu Geschäftsvorfällen enthalten) aufbewahrungspflichtig sein. Genügen die Cloud Leistungen nicht den Anforderungen der Finanzämter, drohen bspw. Bußgelder oder eine Steuerschätzung.

Kontrollfragen:
- Entsprechen die Cloud Leistungen den Anforderungen des § 146 Abs. 2 AO, d. h. stehen die Server des Cloud Anbieters in Deutschland? Falls nein, sind die Voraussetzungen für eine Bewilligung der Finanzbehörden nach § 146 Abs. 2a AO erfüllt?
- Erfüllt der Cloud-Dienst das Erfordernis der Revisionssicherheit nach § 146 Abs. 4 AO?
- Erfolgt die Verarbeitung der Daten im Einklang mit den Anforderungen des § 146 Abs. 5 AO bzw. § 257 Abs. 3 HGB und den „Grundsätzen ordnungsgemäßer Buchführung (GoBS)"?
- Entspricht die Verarbeitung der Daten den „Grundsätzen zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)"? Ist der Datenzugriff in allen drei vorgeschriebenen Zugriffsarten gewährleistet? Erlaubt das Cloud-Angebot eine Kennzeichnung/Trennung der für die Prüfung relevanten und irrelevanten Unterlagen?
- Ist eine Prüfbarkeit der Daten nach den Prüfungsstandards des IDW gewährleistet (u. a. IDW PS 330 – „Abschlussprüfung bei Einsatz von Informationstechnologie")? Ist der Cloud-Anbieter in Zweifelsfragen für Wirtschaftsprüfer des Kunden ansprechbar?
- Gewährleistet der Cloud-Anbieter die Einhaltung der gesetzlich erforderlichen Aufbewahrungsfristen für Unterlagen (§§ 147 Abs. 3 AO, 257 Abs. 4, 5 HGB)?

5 Datensperrung und -beschlagnahme

Im Zusammenhang mit behördlichen Ermittlungen wie auch im Rahmen förmlicher Beweisermittlungsverfahren, wie sie das US Recht (sog. „Discovery") oder englische Recht (sog. „Disclosure") kennen, kann der der Sicherung der Integrität der in der Cloud befindlichen Daten eine hohe Bedeutung zukommen. Sollten diese verändert oder gelöscht werden oder in sonstiger Weise nicht verfügbar sein, drohen empfindliche Sanktionen. Die Nutzung von Cloud Leistungen kann dann zwar einerseits hilfreich sein, weil benötigte zusätzliche Rechenleistung bzw. Speicherkapazität leicht beschafft werden kann. Andererseits darf die Nutzung von Cloud Leistungen die Analyse und Bereitstellung der Informationen nicht erschweren oder gar vereiteln.

Kontrollfragen:
- Bietet der Cloud Anbieter eine Funktion, bestimmte oder alle Daten gezielt vor einer Manipulation oder Löschung in den genannten Situationen zu schützen (z. B. durch entsprechenden Rechteentzug für Mitarbeiter des Cloud Kunden)? Haftet der Cloud Anbieter unabhängig hiervon (möglichst unbeschränkt), falls es durch sein Verschulden zu einer Sanktionierung des Cloud Kunden kommt?
- Kann der Cloud Kunde bestimmte oder alle Daten selektieren und dann gesammelt und in strukturierter Form herunterladen? Gibt es eine Schnittstelle, über die z. B. eine Analysesoftware auf die in der Cloud gespeicherten Daten des Cloud Kunden zugreifen kann?
- Ist das System des Cloud Anbieters leistungsfähig genug, auch umfangreiche Suchaktionen bzw. Datenoperationen zu verkraften? Kann die Kapazität (z. B. Bandbreite) kurzfristig erhöht werden?

6 Exportkontrolle

Die Nutzung von Cloud Leistungen, etwa von E-Mail- oder Dokumentensharing-Software, kann u. U. eine direkte oder indirekte Ausfuhr i. S. d. AWG darstellen und damit einer Genehmigungspflicht unterfallen. Verstöße sind mit Bußgeld oder Haftstrafen bedroht. Kritisch sind z. B. Daten aus dem Bereich Telekommunikation, Chemie, und selbstverständlich Rüstungstechnik. In den Verträgen ist oft nur ein außerordentliches Kündigungsrecht des Cloud Anbieters für den Fall geregelt, dass der Cloud Kunde die Cloud für Zwecke nutzt, die nach Ansicht des Cloud Anbieters gegen Exportkontrollvorschriften, meistens die der USA, verstoßen.

Kontrollfragen:
- Ist sichergestellt, dass die Cloud Leistungen nur für ausfuhrrechtlich unproblematische Daten verwendet werden? Falls nein, ist (auf Grund der Server-Standorte des Cloud Anbieters) sichergestellt, dass es zu keiner Ausfuhr i. S. d. AWG kommt?
- Welche Rechtsfolgen sieht der Vertrag vor, wenn der Exportkontrolle unterliegende Daten verwendet werden?

7 Sonderfall Berufsgeheimnisträger

Berufsgeheimnisträger wie z. B. Ärzte, Psychologen, Rechtsanwälte, Steuerberater und Versicherungsmitarbeiter sind teils durch berufsrechtliche Sonderregelungen, zumindest aber durch § 203 StGB zur besonderen Geheimhaltung der ihnen anvertrauten Informationen verpflichtet. Dies verbietet es grundsätzlich, jedwedem Dritten außerhalb des eigenen Unternehmens bzw. Praxis oder Kanzlei Zugriff auf diese Informationen zu gewähren. Zwar gibt es Bemühungen der einschlägigen Berufsverbände, diese strengen Anforderungen zu lockern, bislang gilt jedoch die bisherige Rechtlage um § 203 StGB fort.
Cloud Computing ist für diese Gruppen daher bislang nur dann möglich, wenn der Kunde ausdrücklich die Weitergabe der Daten an den Cloud Anbieter erlaubt, oder wenn der Cloud Kunde darauf vertraut, es reiche aus, die Daten durchweg verschlüsselt an den Cloud-Anbieter weiterzugegeben und dort verschlüsselt zu speichern.

8 Sonderfall Banken/Versicherungen

Banken und Finanzdienstleister müssen bei Auslagerungen besondere Anforderungen beachten, die sich insbesondere aus § 25a KWG ergeben. Ähnliche Regelungen gelten für den Wertpapierhandel, § 33 WpHG, und Investmentfonds, § 16 InvG, sowie für Versicherungen, § 64a VAG. Dazu finden ergänzend die bankenaufsichtlichen bzw. versicherungsaufsichtlichen „Mindestanforderungen an das Risikomanagement – MaRisk“ der BaFin Anwendung. Grob zusammengefasst enthalten diese Regelungen Vorgaben für die Auslagerung wesentlicher Geschäftsprozesse auf einen Dritten und für die Nutzung von IT-Systemen. Auslagerungsverträge müssen insbesondere eine enge Kontrolle des Auftragnehmers ermöglichen, etwa durch Weisungsrechte, vorgeschriebene Sicherheitsmaßnahmen oder Beendigungsrechte zugunsten des Auftraggebers. Cloud Kunden sollten daher sorgfältig prüfen, ob der Cloud Anbieter und das zugrundeliegende Vertragswerk diesen Anforderungen genügt.

9 Weitere Informationen

Zur weiteren Information über wirtschaftliche und rechtliche Aspekte des Cloud Computing aus der Perspektive von Compliance-Risiken verweisen wir auf die folgenden Quellen, die alle online kostenlos abrufbar sind:

- Bitkom e. V.: „Leitfaden Cloud Computing – Was Entscheider wissen müssen“ (Stand: Ende 2010) (online abrufbar unter http://bit.ly/10lSNel)
- Article 29 Data Protection Working Party: „Opinion 05/2012 on Cloud Computing“, 1.7.2012 (online abrufbar unter http://bit.ly/LuGOC4)
- Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder: „Orientierungshilfe – Cloud Computing“, 26.9.2011 (online abrufbar unter http://bit.ly/nIbMpa)
- EuroCloud Deutschland_eco e. V.: „Leitfaden Cloud Computing – Recht, Datenschutz & Compliance“, 2.12.2010 (kann per E-Mail an leitfaden-recht@eurocloud.de kostenlos im PDF-Format angefordert werden)
- Bundesamt für Sicherheit in der Informationstechnik (BSI): Eckpunktepapier Sicherheitsempfehlungen für Cloud Computing Anbieter, Februar 2012 (online abrufbar unter http://bit.ly/mtxiXW)
- European Network and Information Security Agency (ENISA): Cloud Computing: Benefits, Risks and Recommendations for Information Security, November 2009 (online abrufbar unter http://bit.ly/CLeIX)

AUTOREN

Dr. Jochen Notholt *ist selbstständiger Rechtsanwalt in München. Er ist auf die Beratung von Unternehmen im IT- und Datenschutzrecht spezialisiert.*

Udo Steger *ist Rechtsanwalt und berät zu den Themen IT-Recht, Datenschutz und Open Source. Derzeit ist er in der Rechtsabteilung von Siemens Enterprise Communications in München tätig.*